Общество с ограниченной ответственностью «ОНЛАНТА КОД ИТ»

Программное обеспечение «ONPLATFORM»

Инструкция по установке

Москва 2023 г.

Аннотация

Настоящий документ содержит описание порядка установки и начальной настройки программного обеспечения «ONPLATFORM» – программной платформы, разработанной ООО «ОНЛАНТА КОД ИТ» (далее – Платформа).

Содержание

1 Общие сведения 4
1.1 Наименование 4
1.2 Разработчик 4
1.3 Перечень терминов, определений и сокращений 4
2 Краткое описание программного обеспечения 6
2.1 Назначение Платформы 6
2.2 Состав дистрибутива 7
2.3 Требования к техническому обеспечению Платформы 10
2.3.1 Техническое обеспечение сервера Платформы 10
2.3.2 Техническое обеспечение рабочего места пользователя 10
3 Порядок установки 11
3.1 Подготовка к установке Платформы 11
3.1.1 Подготовка и настройка окружения для установки Платформы 11
3.1.2 Создание управляющей машины 11
3.1.3 Установка ПО, необходимого для развертывания Платформы 13
3.1.3.1 Подготовка виртуальных машин. 13
3.1.3.2 Подготовка Ansible 13
3.2 Развертывание модулей Платформы 18
4 Получение технической поддержки 20

1 Общие сведения

1.1 Наименование

Полное наименование: Программное обеспечение «ONPLATFORM».

Условное обозначение: Платформа.

1.2 Разработчик

Общество с ограниченной ответственностью «ОНЛАНТА КОД ИТ» (ООО «ОНЛАНТА КОД ИТ»)

Фактический адрес: 129075, г. Москва, Мурманский проезд, д. 14, стр. 5

kodit@onlanta.ru; https://onkodit.ru

Тел./факс: +7 (495) 258 89 86

1.3 Перечень терминов, определений и сокращений

Термин	Описание
Деплой	Процесс установки/обновления программного обеспечения в среде Kubernetes
Нода (узел)	Точка в сети, которая либо распределяет данные между другими узлами (нодами) сети, либо является конечной точкой сети
СВАС	Система виртуализации аппаратных средств - любая система виртуализации, в том числе могут использоваться системы из Реестра отечественного программного обеспечения, такие как Скала-Р, Астра Брест и т.д.
Виртуализация	Предоставление набора вычислительных ресурсов или их логического объединения, абстрагированное от аппаратной реализации, и обеспечивающее при этом логическую изоляцию друг от друга вычислительных процессов, выполняемых на одном физическом ресурсе.
ОС	Операционная система
ПО	Программное обеспечение
ППО	Прикладное программное обеспечение
СПО	Системное программное обеспечение
BGP	Протокол динамической маршрутизации, который

Термин	Описание
	относится к классу протоколов маршрутизации внешнего шлюза EGP
CSI-драйвер	Container Storage Interface Компонент, обеспечивающий управление выделением томов (PV) оркестратором Kubernetes
DNS	Domain Name System Сервис, обеспечивающий возможность использования доменных имён вместо IP-адресов, а также корректную работу служб Платформы в условиях динамического выделения IP-адресов
GitOps	Подход, при котором состояние целевой системы (в данном случае, кластера Kubernetes) хранится в репозитории Git и обновляется автоматически при появлении изменений в этом репозитории
IDM	IDentity Manager Сервис, обеспечивающий централизованное хранение информации об учётных записях пользователей и их правах на пользование службами Платформы, а также удостоверяющий пользователей при входе в соответствующие службы
Ingress-контроллер	Отвечает за создание и изменение ресурсов Application Load Balancer
Kea DHCP-сервер	Включает в себя полнофункциональную реализацию сервера с поддержкой протоколов DHCPv4 и DHCPv6. Основан на технологиях BIND 10 и построен с использованием модульной архитектуры
Kubernetes	Программный комплекс, обеспечивающий функционал управления контейнерными средами на одной или нескольких нодах
LINSTOR-контроллер	Основной контроллер, который предоставляет API для создания и управления ресурсами
Mozilla SOPS	Инструмент управления секретами с открытым исходным кодом
Pod	Набор из одного или более контейнеров для совместного развертывания на ноде, реализующий какую-либо функцию
PV	Persistent Volume Логический том в кластере Kubernetes для хранения данных между перезапусками контейнеров
PVC	Persistent Volume Claim

Термин	Описание
	Привязка логического тома (PV) к конкретному приложению в кластере Kubernetes для хранения данных между перезапусками контейнеров
Service Mesh	Компонент, обеспечивающий виртуальную сеть внутри кластера Kubernetes для обеспечения безопасности передаваемых данных, мониторинга обмена данными
SNAT	Замена адреса источника при прохождении пакета в одну сторону и обратной замене адреса назначения в ответном пакете
SSL	Secure Sockets Layer Протокол, обеспечивающий безопасность соединений и обеспечивающий гарантированную сохранность информации, передаваемой по сетям связи, от считывания и модификации путём шифрования передаваемых данных
VPN	Virtual Private Network защищённый канал связи, обеспечивающий безопасный обмен данными между клиентом и Платформой

2 Краткое описание программного обеспечения

2.1 Назначение Платформы

Платформа предназначена для автоматизации процессов разработки ПО путем развертывания и последующего обслуживания рабочих кластеров Kubernetes с интегрированными дополнительными модулями.

Платформа предлагает готовые решения для типовых задач в области автоматизации сборки, поставки приложений в целевые окружения, управления конфигурациями, обеспечения информационной безопасности, мониторинга и диагностики, снижая, таким образом, затраты, связанные с внедрением систем для решения подобных задач и позволяя компаниям сосредоточиться на развитии собственных программных продуктов.

2.2 Состав дистрибутива

Программное обеспечение, используемое Платформой, имеет открытый исходный код. Перечень ПО, используемого Платформой и включенного в состав дистрибутива:

Модуль	ПО

Модуль	ПО
Kubernetes	• Calico. Плагин для Kubernetes, реализующий виртуальную оверлейную сеть и распределенный фаервол для организации и контроля сетевого взаимодействия между контейнеризованными приложениями, запущенными в Kubernetes; • Keda. ПО, реализующее декларативный программный интерфейс для управления автоматическим масштабированием ППО, запущенном в кластерах Kubernetes; • Kubernetes. ПО для оркестрации контейнеризованных приложений: автоматизации их развёртывания, масштабирования и координации; • LINSTOR. Программно-определяемое распределенное хранилище данных, реализующее поддержку персистентного хранения данных СПО и ППО, запущенным в кластерах Kubernetes; • Linkerd. ПО, реализующее сервисную сеть (service mesh) для управления взаимодействием между сервисами (приложениями) в распределенной системе; • MetalLB. ПО, реализующее декларативный программный интерфейс для управления сетевым трафиком, входящим в кластеры Kubernetes; • cert-manager. ПО, реализующее декларативный программный интерфейс для управления выпуском TLS-сертификатов для использования в различном СПО и ППО, запущенном в кластерах Kubernetes; • containerd. Контейнерная среда, используемая Kubernetes для запуска контейнеров; • etcd. Распределенное хранилище конфигурационных данных для Kubernetes и прочих систем; • ingress-nginx. ПО, реализующее декларативный программный интерфейс для управления обработкой входящих запросов к СПО и ППО, развернутому в кластерах Kubernetes; • Docker. ПО для контейнеризации, используемое для запуска отдельных инфраструктурных компонентов Платформы; • Kea. ПО, используемое для организации DHCP-сервера для нужд Платформы. • Nginx. Веб-сервер и прокси-сервер для Unix-подобных систем.
Безопасность	• Dex IDP. ПО, позволяющее использовать информацию о пользовательских учетных записях, хранящуюся на серверах каталогов (LDAP), для аутентификации пользователей в Kubernetes; • FreeIPA. Сервер каталогов (LDAP), а также

Модуль	ПО
	программный и визуальный интерфейс для централизованного управления пользователями платформенных сервисов; • HashiCorp Vault. Распределенное хранилище данных, чувствительных к компрометации (пароли, ключи, токены и т.д.); • Kyverno. ПО, реализующее декларативный программный интерфейс для управления политиками безопасности, применяющимися к СПО и ППО, запущенному в кластерах Kubernetes; • SELinux. Встроенный механизм контроля доступа, реализованный на уровне ядра. Определяет политики доступа к приложениям, процессам и файлам; • Sysdig Falco. ПО для аудита событий на уровне ОС, СПО и ППО; • CFSSL. CloudFlare SSL, удостоверяющий центр в составе Платформы.
Мониторинг	• Alertmanager. ПО, предоставляющее декларативный программный интерфейс для управления правилами генерации и отправки оповещений по данным из централизованного хранилища метрик; • Grafana. ПО для для визуализации и анализа данных, находящихся в централизованном хранилище метрик; • Prometheus. Агрегатор и централизованное хранилище метрик, агрегируемых с уровней ОС, СПО и ППО; • Prometheus Operator. ПО, реализующее декларативный программный интерфейс для управления экземплярами Prometheus, запускаемыми внутри кластеров Kubernetes; • VictoriaMetrics. Централизованное долгосрочное хранилище метрик; • Karma. ПО, предоставляющее веб-интерфейс для просмотра активных событий; • kube-state-metrics. ПО, реализующее функционал сбора метрик мониторинга состояния кластеров Kubernetes; • metrics-server. ПО, реализующее сбор информации о потреблении ресурсов CPU/RAM приложениями в кластере Kubernetes. • CPU-hiccup. Расширенный по функциональности экспортер метрик мониторинга. • Jaeger. ПО для агрегации данных распределенной трассировки запросов, генерируемых СПО и ППО, запущенным в кластерах Kubernetes.

Модуль	ПО
Мониторинг *(логирование)*	• Amazon OpenDistro/OpenSearch (Logstash, OpenSearch, Kibana). Централизованное хранилище диагностических данных из разных источников (например, из журналов событий на уровне ОС, СПО и ППО), а также набор инструментов для визуализации и анализа накопленных данных; • DataDog Vector. ПО для организации сбора событий из различных журналов на уровне ОС, СПО и ППО и отправки этих данных в централизованное хранилище.
Деплой *(конвейер CI/CD)*	• Flagger. ПО, реализующее поддержку продвинутых сценариев деплоя (blue/green, canary) в Kubernetes; • Flux. ПО, реализующее декларативный программный интерфейс для автоматизации установки СПО и ППО в кластерах Kubernetes; • GitLab. Менеджер Git-репозиториев и CI/CD-сервер; • Helm. Пакетный менеджер, реализующий метод упаковки СПО и ППО для развертывания в кластерах Kubernetes; • Nexus OSS. Менеджер репозиториев.
Администрирование *(управление инфраструктурой и Платформой)*	• AlmaLinux. Свободно распространяемый дистрибутив Linux; • Ansible. ПО для автоматизации конфигурирования ОС и СПО; • HashiCorp Terraform. ПО для автоматизации управления виртуальной и сетевой инфраструктурой; • PowerDNS. DNS-сервер для Unix-подобных систем. Может получать DNS-информацию из различных источников данных. Используется для организации балансировки DNS-трафика. • DNS-inventory. Инструмент, обрабатывающий наборы атрибутов хоста для создания инвентаризационного файла Ansible. • Onadm. Утилита, которая на текущий момент скачивает обновленные версии свободного ПО из Интернета и после сборки размещает их во внутреннем хранилище пакетов Платформы.
Kubernetes data plane *(резервное копирование)*	• MinIO. Распределенное объектное хранилище данных с программным интерфейсом, совместимым с Amazon S3; • Velero. ПО, реализующее декларативный программный интерфейс для управления резервным копированием данных, генерируемых СПО и ППО, запущенным в кластерах Kubernetes.

2.3 Требования к техническому обеспечению Платформы

2.3.1 Техническое обеспечение сервера Платформы

Минимальные требования к серверному оборудованию для размещения Платформы, без учета мощностей, требуемых для размещения полезной нагрузки (kubernetes worker):

Процессор	44 vCPU Минимум Intel Xeon (Broadwell E5-2686 v4 или Haswell E5-2676 v3) 2.4 Ггц
Оперативная память	Минимум 54 Гб
Жесткий диск	Не менее 266 Гб SAS, Не менее 128 Гб SSD
Сетевое окружение	Средняя сетевая задержка в пределах локальной сети передачи данных не более 1 мс.
Пропускная способность Интернет-канала	Не менее 100 Мбит/с

2.3.2 Техническое обеспечение рабочего места пользователя

Рабочее место пользователя Платформы должно отвечать следующим требованиям:

- наличие возможности удаленного доступа к инфраструктуре, на которой развернута Платформы;
- наличие доступа в сеть Интернет – скорость не менее 10 Мбит;
- наличие SSH-клиента – SSH-доступ по ключу до узла, являющегося Master-узлом кластера;
- наличие VPN-клиента – подключение к внутренней платформенной сети передачи данных с помощью VPN-клиента WireGuard.

3 Порядок установки

3.1 Подготовка к установке Платформы

3.1.1 Подготовка и настройка окружения для установки Платформы

Платформа поддерживает развертывание в окружениях с поддерживаемыми СВАС.

Поддерживаемая ОС для серверов - AlmaLinux 8.6;

При развертывании Платформы необходимо провести подготовку:

- Выделить вычислительные ресурсы необходимые для размещения ВМ платформы

- создать учетную запись в CBAC с административными правами для текущей инсталляции Платформы;
- если планируется использовать BGP для анонсирования маршрутов для виртуальных адресов, использующихся в Kubernetes, необходимо также проверить корректность настройки следующих параметров:
    - созданной учетной записи пользователя присвоено право изменения параметров динамической маршрутизации.
- создать сеть для организации, в которой будут находиться все виртуальные машины Платформы, получающие свои адреса по DHCP, поэтому в ней должно быть разрешено использование сторонних DHCP-серверов;
- создать правила фаервола, разрешающие любой исходящий трафик для созданной сети организации, а также создать SNAT-правило для обеспечения доступа в Интернет из этой сети. В SNAT-правиле в качестве External IP следует указать адрес, присвоенный основному внешнему интерфейсу маршрутизатора, а в качестве Internal IP - подсеть, выбранную для сети организации (в CIDR-нотации);
- загрузить в библиотеку шаблонов шаблон виртуальной машины, который будет использоваться для создания всех машин Платформы. Шаблон должен быть построен на основе одной из версий ОС, поддерживаемых Платформой.

Вся необходимая информация для работы с Платформой передается пользователю до начала развертывания Платформы.

3.1.2 Создание управляющей машины

Управляющая машина, с которой будет производиться развертывание Платформы с помощью средств автоматизации, должна создаваться с учетом следующих особенностей:

- в качестве ОС должна использоваться последняя поддерживаемая версия AlmaLinux 8.6[1];
- управляющая машина должна быть подключена к той же сети организации, в которой планируется расположить остальные виртуальные машины Платформы;
- созданной управляющей машине нужно присвоить статический IP-адрес. Обычно используется четвертый адрес в платформенной сети. Например, если для Платформы выбрана сеть 10.255.0.0/22 (по умолчанию), то управляющей машине может быть присвоен IP-адрес 10.255.0.3 (адрес 10.255.0.2 в этом случае будет использован DNS/DHCP-сервером). Если инсталляция Платформы предполагает использование высокодоступных DNS/DHCP-серверов, то адрес управляющей машины должен быть выбран таким образом, чтобы находиться после адресов, предназначенных для DNS/DHCP серверов. Например, если DNS/DHCP серверам выделены

1 актуальная версия на момент создания документа

адреса 10.255.0.2 и 10.255.0.3, то управляющей машине следует присвоить IP-адрес 10.255.0.4.

Для корректной работы созданной управляющей машины нужно выполнить следующие действия:

- создать личную учетную запись пользователя для сотрудника, который будет производить развертывание Платформы. Аутентификация должна осуществляться строго по SSH-ключу. Пароль для личной учетной записи должен быть заблокирован (passwd -l <user>). Пользователя с данной учетной записью следует сразу добавить в группу wheel и разрешить для этой группы выполнение любых команд через sudo без ввода пароля;
- Скачать дистрибутив платформы из официального репозитория repo.onlanta.ru onplatform-ansible-<версия>.tar.gz в домашнем каталоге созданной учетной записи пользователя.
- зайти в каталог с распакованным дистрибутивом onplatform-ansible и выполнить команду sudo master.sh. Этот скрипт установит на машину Terraform, Ansible, а также все прочие необходимые для работы с Платформой инструменты. В процессе исполнения скрипта будет сгенерирован GPG-ключ, который будет использоваться для шифрования и расшифровки секретов, хранящихся в файлах Mozilla SOPS. При генерации этого ключа будет запрошен пароль для защиты самого ключа. В ответ на этот запрос следует ввести алфавитно-цифровой, регистрозависимый пароль длиной в 32 символа. Этот пароль, а также файл /etc/ansible/gpg-keys/sops.key, содержащий в себе сгенерированный ключ в зашифрованном виде, необходимо внести в соответствующий проекту раздел корпоративного менеджера паролей, для которого разворачивается Платформа;
- добавить созданную ранее учетную запись пользователя в группы docker, ansible и выполнить повторную авторизацию;
- включить GPG-агент и импортировать GPG-ключ для дальнейшего использования в SOPS.

3.1.3 Установка ПО, необходимого для развертывания Платформы

3.1.3.1 Подготовка виртуальных машин.

Необходимо развернуть на СВАС виртуальные машины из поставленного шаблона в соответствии с перечнем, переданным администратором

3.1.3.2 Подготовка Ansible

Для установки ПО Ansible нужно выполнить следующие шаги:

1) Заполнить домен Платформы и IP-адрес(а) DNS/DHCP серверов в файле «inventory/inventory.yml». Обычно в качестве IP-адреса используется третий адрес в платформенной сети. Например, если для Платформы выбрана сеть 10.255.0.0/22 (то есть по умолчанию), то DNS/DHCP-серверу может быть присвоен IP-адрес

10.255.0.2. Если используется высокодоступная конфигурация платформенного DNS/DHCP сервера, то для второй машины в этом случае может использоваться адрес 10.255.0.3;

2) Заполнить переменные в файле «inventory/group_vars/all.yml»:

Переменная	Комментарий
onplatform_hypervisor	Используемая платформа виртуализации
onplatform_vcd_address	URL для доступа к API CBAC
onplatform_vcd_organization	Имя тенанта CBAC, в котором выделены ресурсы для развертывания платформы.
onplatform_datacenter	Условное обозначение тенанта, в котором располагается текущая инсталляция Платформы. Используется в качестве дополнительной метки для собираемых системой мониторинга метрик
onplatform_inventory	Информация обо всех хостах Платформы. Здесь с самого начала должны быть перечислены все хосты, входящие в текущую инсталляцию Платформы. Для каждого должны быть указано **короткое** имя хоста (**не FQDN**) и набор атрибутов. В шаблоне инвентаря есть образцы записей для всех видов платформенных сервисов. В большинстве случаев достаточно актуализировать этот список, изменив количество и имена хостов
onplatform_domain	Внутренний домен Платформы
onplatform_network	Внутренняя сеть Платформы в CIDR-нотации
onplatform_dhcp_pools	Пулы адресов для использования платформенным DHCP-сервером
onplatform_dns_vip	Виртуальный IP для платформенного DNS (PowerDNS)
onplatform_vault_vip	Виртуальный IP для платформенного хранилища секретов (HashiCorp Vault).
onplatform_logs_vip	Виртуальный IP для платформенного агрегатора логов (OpenSearch)
alertmanager_telegram_chat_id	Идентификатор канала или группы, используемых для рассылки оповещений от платформенной системы мониторинга

3) Заполнить переменные в файлах «inventory/group_vars/<…>_orchestrator_k8s.yml»:

Переменная	Комментарий
k8s_balancer_vip	Виртуальный IP для балансировщика запросов к Kubernetes API этого кластера

Переменная	Комментарий
linstor_controller_vip	Виртуальный IP для контроллеров LINSTOR в этом кластере Kubernetes
k8s_ingress_nginx_lb_ip	Виртуальный IP для основного Ingress-контроллера в этом кластере Kubernetes
k8s_ingress_nginx_system_lb_ip	Виртуальный IP для системного Ingress-контроллера в этом кластере Kubernetes
metallb_peer_address	Адрес пограничного маршрутизатора для установления BGP-сессии (если эта возможность используется)
metallb_peer_asn	Номер автономной системы для пограничного маршрутизатора
metallb_asn	Номер автономной системы для этого кластера Kubernetes
metallb_address_pools	Сетевой диапазон, из которого могут выдаваться адреса для сервисов LoadBalancer в этом кластере Kubernetes
k8s_service_subnet	Сетевой диапазон для оверлейной сети, из которого будут выдаваться адреса для сервисов ClusterIP в этом кластере Kubernetes
k8s_pod_subnet	Сетевой диапазон для оверлейной сети, из которого будут выдаваться адреса для Pods в этом кластере Kubernetes
calico_allow_workload_to_workload	Разрешить исходящий трафик из пользовательских Pods к другим пользовательским Pods. Доступ, разрешенный здесь, нельзя будет запретить с помощью NetworkPolicy в дальнейшем
calico_allow_workload_to_worker_nodes	Разрешить исходящий трафик из Pods к воркер-нодам Kubernetes. Доступ, разрешенный здесь, нельзя будет запретить с помощью NetworkPolicy в дальнейшем
calico_allow_workload_to_lan	Разрешить исходящий трафик из Pods во внутреннюю сеть. Доступ, разрешенный здесь, нельзя будет запретить с помощью NetworkPolicy в дальнейшем
calico_allow_workload_to_wan	Разрешить исходящий трафик из Pods в Интернет. Доступ, разрешенный здесь, нельзя будет запретить с помощью NetworkPolicy в дальнейшем

4) Заполнить секреты в файле «inventory/group_vars/all.sops.yml». Для автоматической генерации секретов там, где это в принципе возможно, нужно запустить скрипт pwgen.sh. Остальные секреты следует заполнить вручную:

Секрет	Комментарий	Генерируется
onplatform_vcd_username	Имя учетной записи CBAC с административными правами	Нет
onplatform_vcd_password	Пароль учетной записи CBAC с административными правами	Нет
pdns_api_password	Пароль для доступа к PowerDNS API	Да
pdns_webserver_password	Пароль для доступа к веб-серверу PowerDNS	Да
kea_ctrl_username	Имя учетной записи администратора Kea DHCP server	Нет
kea_ctrl_password	Пароль учетной записи администратора Kea DHCP server	Да
pki_ca_automation_username	Имя учетной записи администратора внутреннего удостоверяющего центра	Нет
pki_ca_automation_password	Пароль учетной записи администратора внутреннего удостоверяющего центра	Да
freeipa_dc_password	Пароль администратора LDAP (cn=Directory Manager) FreeIPA	Да
freeipa_admin_password	Пароль учетной записи администратора по умолчанию (admin) FreeIPA	Да
vault_bind_username	Имя учетной записи для работы HashiCorp Vault с LDAP-сервером	Нет
vault_bind_password	Пароль учетной записи для работы HashiCorp Vault с LDAP-сервером	Да
nexus_admin_password	Пароль учетной записи администратора по умолчанию (admin) Sonatype Nexus	Да
nexus_onplatform_password	Пароль учетной записи платформенного пользователя по умолчанию (onplatform) Sonatype Nexus	Да
nexus_bind_username	Имя учетной записи для работы Sonatype Nexus с LDAP-сервером	Нет
nexus_bind_password	Пароль учетной записи для работы Sonatype Nexus с LDAP-сервером	Да
gitlab_bind_username	Имя учетной записи для работы GitLab	Нет

Секрет	Комментарий	Генерируется
	с LDAP-сервером	
gitlab_bind_password	Пароль учетной записи для работы GitLab с LDAP-сервером	Да
gitlab_root_password	Пароль учетной записи первичного администратора (root) GitLab	Да
gitlab_admin_password	Пароль учетной записи администратора по умолчанию (gitlab-admin) GitLab	Да
grafana_admin_password	Пароль учетной записи администратора по умолчанию (admin) Grafana	Да
grafana_bind_username	Имя учетной записи для работы Grafana с LDAP-сервером	Нет
grafana_bind_password	Пароль учетной записи для работы Grafana с LDAP-сервером	Да
alertmanager_telegram_bot_token	Токен для Telegram-бота, используемого для рассылки оповещений от платформенной системы мониторинга	Нет
opensearch_bind_username	Имя учетной записи для работы OpenSearch с LDAP-сервером	Нет
opensearch_bind_password	Пароль учетной записи для работы OpenSearch с LDAP-сервером	Да
opensearch_security_admin_password	Пароль учетной записи администратора по умолчанию (admin) OpenSearch	Да
opensearch_security_kibana_password	Пароль учетной записи kibanaserver в OpenSearch	Да
opensearch_security_logstash_password	Пароль учетной записи logstash в OpenSearch	Да
opensearch_jaeger_agent_username	Имя учетной записи для подключения агентов Jaeger к Opensearch	Нет
opensearch_jaeger_agent_password	Пароль учетной записи для подключения агентов Jaeger к OpenSearch	Да

5) Заполнить секреты в файлах «inventory/group_vars/<…>_orchestrator_k8s.sops.yml». Для автоматической генерации секретов там, где это в принципе возможно, нужно запустить скрипт pwgen.sh. Остальные секреты следует заполнить вручную:

Секрет	Комментарий	Требования
k8s_admin_username	Имя учетной записи администратора по умолчанию для текущего кластера Kubernetes	Нет
k8s_admin_password	Пароль учетной записи администратора по умолчанию для текущего кластера Kubernetes	Да
k8s_flux_git_username	Имя учетной записи GitLab для подключения Flux к GitOps-репозиторию	Нет
k8s_flux_git_password	Пароль учетной записи GitLab для подключения Flux к GitOps-репозиторию	Да
metallb_memberlist_key	Ключ для кластерной группы MetalLB Speaker	Да
k8s_encryption_initial_key	Ключ для шифрования данных в etcd-кластере	Да
k8s_dex_bind_username	Имя учетной записи для работы Dex с LDAP-сервером	Нет
k8s_dex_bind_password	Пароль учетной записи для работы Dex с LDAP-сервером	Да
k8s_dex_k8s_authenticator_client_secret	Ключ для клиента Dex (dex-k8s-authenticator)	Да
k8s_linkerd_viz_auth_client_secret	Ключ для клиента Dex (Linkerd)	Да
k8s_linkerd_viz_auth_cookie_secret	Ключ для клиента Dex (Linkerd)	Да
k8s_jaeger_auth_client_secret	Ключ для клиента Dex (Jaeger)	Да
k8s_jaeger_auth_cookie_secret	Ключ для клиента Dex (Jaeger)	Да

6) Зашифровать заполненные файлы SOPS с помощью ключа, сгенерированного при выполнении первичной настройки управляющей машины скриптом «master.sh».

3.2 Развертывание модулей Платформы

Модули Платформы разворачиваются на предварительно созданных ВМ с помощью Ansible.

При создании сети Платформы, после разворачивания DNS/DHCP серверов, на управляющей машине нужно указать адреса развернутых DNS-серверов в параметрах основного сетевого соединения.

При развертывании хранилища секретов нужно с любой виртуальной машины кластера хранилища секретов забрать содержимое файла /dev/shm/onplatform-vault.tmp и удалить этот файл на всех виртуальных машинах кластера. Содержимое этого файла необходимо внести в соответствующий проекту раздел корпоративного менеджера паролей, для которого разворачивается Платформа. В нем содержится первичный корневой токен Vault (initial root token) и ключи для расшифровки хранилища Vault (unseal keys).

После развертывания всех модулей Платформы, нужно установить агенты для сбора метрик и логов на все виртуальные машины.

4 Получение технической поддержки

Для получения консультаций по вопросам, связанным с установкой Платформы, необходимо обратиться в службу технической поддержки следующими способами:

- связаться по телефону +7 (495) 258 89 86 (рабочие дни с 09:00 до 18:00 по московскому времени);
- связаться по электронной почте kodit@onlanta.ru.

Все поступившие в службу технической поддержки обращения пользователей регистрируются в ITSM-системе производителя Платформы.

В тексте обращения, направленного в службу технической поддержки, необходимо указать наименование пользователя Платформы, номер лицензии, контактный телефон, а также подробно описать возникшую ситуацию (в т. ч. прикрепить скриншоты экрана и т. п.).